REMARKS

Reconsideration of the present application, as amended, is respectfully requested. Claims 1, 13 and 24 have been amended.

Examiner rejected claims 10-12 and 24-26 under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,310,966 to Dulude et al. Examiner rejected claims 1-4, 6-9, 22, and 23 under 35 U.S.C. §103(a) as being unpatentable over Dulude in view of U.S. Patent No. 5,535,276 to Ganesan. Examiner rejected claim 5 under 35 U.S.C. §103(a) as being unpatentable over Dulude and Ganesan as applied to claim 1 above, and further in view of U.S. Patent No. 5,867,578 to Brickell et al. Examiner rejected claims 13-21 under 35 U.S.C. §103(a) as being unpatentable over Dulude in view of U.S. Patent No. 6,587,946 to Jakobsson.

Claims 10-12

Examiner rejected claims 10-12 under 35 U.S.C. §102(e) as being anticipated by Dulude. Claim 10 recites:

> A method of providing a certificate from a client to a third party server, the method comprising:
> receiving a request for a certificate from the third party server;
> forwarding the request to a biometric certification server (BCS);
> and forwarding the biometric identification to the BCS receiving a biometric identification from the client;
> if the biometric identification matches a registered user on the BCS, receiving a certificate including a public key of the client certified by the BCS; and
> forwarding the certificate to the third party server, thereby identifying the client to the third party server.

(Emphasis Added). In contrast, Dulude discloses a biometric certification system associated with a network, which receives biometric input from a user and compares the input with biometric data that is pre-stored either in a biometric database or in smart

cards. (Dulude, col. 5, lines 35-41). Dulude's system returns a decision, in the form a validation signal, which indicates whether the validation was successful, or a percentage certainty in the validation match. (Dulude, column 7, lines 58-67. Dulude does not teach or suggest forwarding the certificate to the third party server, thereby identifying the client to the third party server. The Examiner asserts that Dulude discusses sending a the certificate to the server, and references Dulude, column 6, lines 50-65. However, in the referenced section of Dulude simply discusses sending a biometric certificate to the biometric certificate extractor, for analysis. Note that in Dulude, the biometric certificate extractor and associated analysis system corresponds to the BCS of claim 10. Therefore, Dulude does not teach or suggest sending the certificate to a third party server, as recited in claim 10, as amended.

Accordingly, independent claim 10 and its dependent claims 11-12 are not anticipated by Dulude.

Claims 24-26

Examiner rejected claims 24-26 under 35 U.S.C. §102(e) as being anticipated by Dulude. Claim 24 recites:

> An apparatus, comprising:
> a crypto-server having a crypto-proxy interface for receiving a request for a cryptographic function from a client on a secure connection;
> an authentication engine to authenticate a user based on biometric data;
> a cryptographic engine to use the user's private key, as a virtual smart card, to perform a requested cryptographic function; and
> the crypto-proxy interface for returning data to the client, after the cryptographic functions are performed.

(Emphasis Added). As discussed above, Dulude does not teach or suggest a cryptographic engine to use the user's private key, as a virtual smart card, to perform a

requested cryptographic function. The Examiner uses the language from the pending claims, and points to most of the detailed description, but Applicant fails to identify a logical element within Figure 5, or the associated description of Dulude that would correspond to a cryptographic engine to use the user's private key, as a virtual smart card, to perform a requested cryptographic function.

Accordingly, independent claim 24 and its dependent claims 25-26 are not anticipated by Dulude.

Claims 1-4, 6-9

Examiner rejected claims 1-4, and 6-9 under 35 U.S.C. §103(a) as being unpatentable over Dulude in view of Ganesan. Applicant respectfully submits that this combination does not teach each and every element of these claims.

Ganesan discusses securing communications using split private key asymmetric cryptography. Ganesan does not teach or suggest a biometric certification server generating a disposable key pair, to perform a cryptographic service.

Claim 1 recites:

> A method of providing remote cryptographic services, the method comprising:
> a client requesting a cryptographic service;
> establishing a secure connection between the client and a biometric certification server (BCS);
> receiving biometric data from a user;
> the BCS generating a disposable public key/private key pair if the user is authenticated based on the biometric data; and
> the BCS performing the requested cryptographic service.

(Emphasis Added). As discussed above, Dulude does not teach or suggest a biometric certification server to perform a requested cryptographic service, and Ganesan does not supply this missing element.

Since the combination of Dulude and Ganesan does not teach or suggest a biometric certification server performing a requested cryptographic service as claimed in independent claim 1, the combination cannot be interpreted to render obvious Applicant's invention as claimed in claims 1-4, and 6-9. Accordingly, Applicant respectfully requests the withdrawal of the rejection over this combination.

Claim 22

Examiner rejected claim 22 under 35 U.S.C. §103(a) as being unpatentable over Dulude in view of Ganesan. Applicant respectfully submits that this combination does not teach each and every element of claim 22.

Claim 22 recites:

> An apparatus for permitting remote cryptographic functions comprising:
> a crypto-API (application program interface) for receiving cryptographic function requests;
> a cryptographic service provider for establishing a secure connection to a remote crypto-server, and having the crypto-server perform the cryptographic function; and
> a sensor for receiving biometric data from a user, the biometric data sent to the crypto-server to authenticate the user, the remote crypto-server to generate a disposable public key/private key pair and perform the requested cryptographic function when the user is successfully authenticated using the biometric data.

(Emphasis Added). As discussed above, as neither Dulude nor Ganesan teach or suggest a crypto-server to perform a requested cryptographic function, once the user is authenticated using the biometric data. Rather, Dulude teaches only the use of the

biometric data for authentication, but does not teach or suggest a crypto-server to perform a function after successful authentication. Accordingly, Applicant respectfully requests the withdrawal of the rejection over this combination.

Claim 23

Examiner rejected claim 23 under 35 U.S.C. §103(a) as being unpatentable over Dulude in view of Ganesan. Applicant respectfully submits that this combination does not teach each and every element of claim 23.

Claim 23 recites:

> An apparatus comprising:
> a client comprising:
> a crypto-API (application program interface) for receiving cryptographic function requests; and
> a cryptographic service provider for establishing a secure connection to a remote crypto-server, and having the crypto-server generate a disposable public key/private key pair and perform the cryptographic function; and
> a sensor for receiving biometric data from a user, the biometric data sent to the crypto-server to authenticate the user;
> the remote crypto-server comprising:
> a crypto-proxy interface for receiving a request for the cryptographic function from the client on the secure connection;
> an authentication engine for authenticating the user based on the biometric data;
> a cryptographic engine for performing the cryptographic functions; and
> the crypto-proxy interface for returning data to the client, after the cryptographic functions are performed.

(Emphasis Added). As discussed above, as neither Dulude nor Ganesan teach or suggest a cryptographic engine to perform cryptographic functions, as recited in claim 23. Accordingly, Applicant respectfully requests the withdrawal of the rejection over this combination.

Claim 5

Examiner rejected claim 5 under 35 U.S.C. §103(a) as being unpatentable over Dulude and Ganesan in view of U.S. Patent No. 5,867,578 to Brickell et al. Claim 5 depends on claim 1, and incorporates its limitations. As discussed above, neither Dulude nor Ganesan teaches or suggests a biometric certification server, and Brickell does not supply this missing element.

Brickell discusses a multi-step digital signature method. Brickell does not teach or suggest a biometric certification server to perform a cryptographic function, as recited in claim 1, and therefore in claim 5.

Therefore, Applicant respectfully requests the withdrawal of the rejection over this combination of references.

Claims 13-21

Examiner rejected claims 13-21 under 35 U.S.C. §103(a) as being unpatentable over Dulude in view of U.S. Patent No. 6,587,946 to Jakobsson. Applicant respectfully submits that this combination does not teach each and every element of these claims.

Jakobsson discusses quorum controlled asymmetric proxy cryptography for use in encrypting and decrypting transcripts. Jakobsson does not teach or suggest a cryptographic engine separate from an authentication engine at all.

Claim 13 recites:

> An apparatus for performing remote cryptographic functions comprising: a crypto-server having a crypto-proxy interface for receiving a request for a cryptographic function from a client on a secure connection;

an authentication engine for authenticating the user based on biometric data;

a cryptographic engine for performing the cryptographic functions; and

the crypto-proxy interface for returning data to the client, after the cryptographic functions are performed.

(Emphasis Added). As discussed above, Dulude does not teach or suggest a cryptographic engine, for performing cryptographic functions, and Jakobsson does not supply this missing element.

Since neither Dulude nor Jakobsson teaches a crypto-server as claimed in independent claim 13, Applicant respectfully requests the withdrawal of the rejection over this combination.

Applicant respectfully submits that in view of the amendments and discussion set forth herein, the applicable rejections have been overcome. Accordingly, the present and amended claims should be found to be in condition for allowance.

If a telephone interview would expedite the prosecution of this application, the Examiner is invited to contact Judith Szepesi at (408) 720-8300.

If there are any additional charges/credits, please charge/credit our deposit account no. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: 6/8/05

Judith A. Szepesi
Reg. No. 39,393

Customer No. 08791
12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025
(408) 720-8300